UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON

ANIA VILLALON, individually and on behalf of all others similarly situated, Plaintiff, v. T-MOBILE USA, INC., Defendant.	Case No. _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Ania Villalon ("Plaintiff"), individually and as a class representative for others similarly situated, bring this action against Defendant T-Mobile USA, Inc. ("T-Mobile" or "Defendant"). Plaintiff alleges upon personal knowledge as to her own actions and upon information and belief as to all other matters and believe that reasonable discovery will provide additionally evidentiary for the allegations herein.

I. NATURE OF THE ACTION

1. This class action arises out of the recent cyberattack and data breach that was perpetrated against Defendant T-Mobile, a national telecommunications company that provides mobile telephone services to customers throughout the United States (the "Data Breach"). The Data Breach resulted in unauthorized access and exfiltration of highly sensitiveand personal information (the "Private Information").

2. As a result of the Data Breach, Plaintiff and approximately 40 million former or prospective customers who applied for credit with T-Mobile, approximately 13 million current

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

postpaid customers, and 850,000 active prepaid customers (the "Class Members")[1] suffered present injury and damages in the form of identity theft, out-of-pocket expenses and the value of the time reasonably incurred to remedy or mitigate the effects of the unauthorized access, exfiltration, and subsequent criminal misuse of their sensitive and highly personal information.

3. The Private Information compromised in the Data Breach includes names, phone numbers, drivers' licenses, government identification numbers, Social Security numbers, dates of birth, and T-Mobile account PINs.[2]

4. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained.

5. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer system and network in a condition vulnerable to cyberattacks.

6. The mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from the risk of a ransomware attack.

7. Plaintiff's and Class Members' identities are now at considerable risk because of Defendant's negligent conduct since the Private Information that T-Mobile collected and maintained is now in the hands of data thieves.

8. Plaintiff's and Class Members' Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and its failure to adequately protect the Private Information of its current, former, and prospective clients.

[1] *See* T-Mobile Shares Additional Information Regarding Ongoing Cyberattack Investigation, T-Mobile (Aug. 17, 2021), https://www.t-mobile.com/news/network/additional-information-regarding-2021-cyberattack- investigation (last visited Aug. 24, 2021).

[2] *Id.*

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

9. As a result of the Data Breach, Plaintiff and Class Members are exposed to a heightened present and imminent risk of fraud and identity theft. As a result of Defendant's actions and inactions, as set forth herein, Plaintiff and Class Members must now and in the future closely monitor their financial accounts and information to guard against identity theft, among other issues.

10. Plaintiff and Class Members have and may in the future incur actual monetary costs, including but not limited to the cost of purchasing credit monitoring services, credit freezes, credit reports or other protective measures to deter and detect identity theft.

11. Plaintiff and Class Members have and may in the future expend time spent mitigating the effects of the Data Breach, including time spent dealing with actual or attempted fraud and identity theft.

12. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

13. Accordingly, Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendant's negligence and failure to: (i) adequately protect its customer's Private Information, (ii) warn its current, former, and potential customers of their inadequate information security practices, and (iii) effectively monitor their data systems for security vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

14. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

II. JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

proposed class, and at least one member of the class is a citizen of a state different from Defendant.

16. This Court has personal jurisdiction over Defendant because Defendant has its principal place of business is located in the State of Washington.

17. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to and/or emanated from this District. Defendant resides within this judicial district and a substantial part of the events giving rise to the claims alleged herein occurred within this judicial district.

III. PARTIES

18. Plaintiff Ania Villalon is a citizen of New York, residing in Bronx County, New York and has been a T-Mobile customer for approximately four (4) years.

19. On or about August 16, 2021, Plaintiff Villalon, and the public, was first notified of the Data Breach by T-Mobile and that cybercriminals had illegally accessed and stole confidential customer data from millions of T-Mobile customer accounts. On August 19, 2021, Ms. Villalon received a text message from T-Mobile notifying her that her PII was accessed without her authorization, exfiltrated, and/or stolen in the Data Breach.

20. As a direct and proximate result of the breach, Plaintiff Villalon has made reasonable efforts to mitigate the impact of the breach, including but not limited to: checking bank accounts for any indication of actual or attempted identity theft or fraud, researching the internet concerning this Data Breach; discussing the breach with her friends and family; and reviewing credit reports for any indications of actual or attempted identity theft or fraud. This is valuable time Plaintiff Villalon otherwise could have and would have spent on other activities, including but not limited to work and/or recreation.

21. On August 22, 2021, shortly after T-Mobile announced the Data Breach, Plaintiff Villalon experienced two attempted unauthorized transactions on her PayPal account via her PayPal Cash Card. Said transactions were automatically declined because the transactions were more than what was in Plaintiff's account at that time.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

22. Plaintiff Villalon is very concerned about additional identity theft, her banking account and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

23. Plaintiff Villalon suffered actual injury from having Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Defendant obtained from Plaintiff; (b) violation of Plaintiff's privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

24. Plaintiff Villalon has and will spend a significant amount of time responding to the impacts of the Data Breach. The time spent dealing with the fallout from the Data Breach is time Plaintiff otherwise would have spent on other activities, such as work and/or recreation.

25. As a result of the Data Breach, Plaintiff Villalon anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is and will continue to be at increased risk of identity theft and fraud for years to come.

26. Defendant T-Mobile US, Inc. is a for-profit company incorporated in Delaware with its principal place of business in the State of Washington at 12920 SE 38th St, Bellevue, Washington 98006. Defendant is a wireless network operator and national telecommunications company that provides wireless voice and data services in the United States, Puerto Rico, and U.S. Virgin Islands. Defendant collects and maintains the personal information of millions of customers throughout the United States, including New York and Washington.

27. Defendant is a publicly traded company and in 2020, reported total revenue of $68.4 billion.

VI. FACTUAL ALLEGATIONS

The Data Breach

28. On August 16, 2021, T-Mobile confirmed that it was the subject of a data breach affecting over 100 million customers. This acknowledgement came after a report by Vice.com on

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

August 15, 2021, that an unidentified individual was attempting to sell PII from the T-Mobile server. The PII accessed in the data breach is believed to include customer's names, addresses, social security numbers, driver's license information, phone numbers, dates of birth, and unique IMEI and IMSI numbers. According to Vice.com, the unidentified individual knew T-Mobile became aware of the hack, because he or she eventually lost access to the backdoored servers.

29. On August 17, 2021, T-Mobile released a more detailed statement about the data breach, verifying that the hack did occur and how many customers were affected. Since August 17, 2021, T-Mobile has identified over 10 million more customers whose PII was likely compromised.

30. On August 20, 2021, T-Mobile released another press statement, updating the number of customers likely affected by the data breach. T-Mobile also offered two years of free identity protection services with McAfee's ID Theft Protection Services and free scam-blocking protection through Scam Shield.

The Value of Personally Identifiable Information

31. PII, or personal identifiable information, is data that can be used to detect a specific individual. PII includes name, address, email, telephone number, date of birth, passport number, fingerprint, driver's license number, credit/debit card number, and social security number.

32. It is important to keep PII safe, especially in digital form. PII stored on a computer, phone, or website can be vulnerable to cybercriminals. If a criminal is fraudulently using a user's information, she can become the victim of fraud, identity theft, and/or phishing attacks.

Defendant Was Aware of the Risks of a Data Breach

33. Defendant had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Members of the Classes, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

34. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access

35. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches preceding the date of the breach.

36. Data breaches have become widespread. For example, the United States saw 1,244 data breaches in 2018 and had 446.5 million exposed records.[3]

37. Defendant clearly understood this reality because a quote, posted on Defendant's website, by a senior manager of T-Mobiles Cyber Architecture & Controls unit stated that:

> At T-Mobile, everyone is challenge[d] to think outside of conventional approaches to digital security; all know assumptions are reevaluated. We work on forward-thinking technologies, including micro-segmentation, machine learning, predictive analytics, web situational awareness, advance threat mitigation, active defense, data obfuscation and next-generation endpoint technologies it.[4]

38. However, T-Mobile failed to take fully implement data security systems and protect critical Private Information belonging to consumers.

39. Indeed, data breaches, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry, including Defendant.

40. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[5] Identity thieves use stolen personal information for a variety of crimes, including

---

[3] 98 Must-Know Data Breach Statistics for 2021, Varonis, https://blogvaronis2.wpengine.com/data-breach-statistics/ (last visited Aug. 24, 2021).
[4] Digital Security, T-Mobile, https://www.t-mobile.com/careers/digital-security (last visited Aug. 24, 2021).
[5] *See* Taking Charge, What to Do If Your Identity is Stolen, FTC, 3 (Apr. 2013), https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf (last visited Aug. 24, 2021).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

government benefits fraud, phone or utilities fraud, and bank and finance fraud.[6]

41. The Private Information of Plaintiff and Members of the Classes was taken by hackers to engage in identity theft or and or to sell it to other criminals who will purchase the Private Information for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

42. Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Members of the Classes, including Social Security numbers, driver's license, and/or dates of birth, and of the foreseeable consequences that would occur if Defendant's data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Members of the Classes a result of a breach.

43. Plaintiff and Members of the Classes now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Classes are incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

44. The injuries to Plaintiff and Members of the Classes were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Members of the Classes.

Defendant Failed to Comply with FTC Security Guidelines on Storing and Protecting PII

45. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

[6] *Id*. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *See* Taking Charge, What to Do If Your Identity is Stolen, FTC, 3 (Apr. 2013), https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf (last visited Aug. 24, 2021).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

46. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

47. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

48. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

49. Defendant failed to properly implement basic data security practices, and their failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45. 67. Defendant was at all times fully aware of their obligation to protect the Private Information of current, former, and prospective customers. Defendant was also aware of the significant repercussions that would result from their failure to do so.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

Defendant Failed to Comply with Industry Standards

50. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendant's cybersecurity practices.

51. Best cybersecurity practices that are standard in Defendant's industry include encrypting files; installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

52. Defendant failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC- 1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness.

53. These foregoing frameworks are existing and applicable industry standards in Defendant's industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the Cyber-Attack and causing the Data Breach.

Plaintiff and Class Members Have Suffered Harm and Are at an Increased Risk of Fraud and Identity Theft as a Result of the Data Breach

54. Due to the Data Breach, Plaintiff and Class members have suffered and will continue to suffer harm.

55. Plaintiff and Class members face an increased risk of identity theft, phishing attacks, and related cybercrimes because of the Data Breach. Those impacted are under heightened and prolonged anxiety, as they will be at risk for falling victim to cybercrimes for years to come.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

56. As a result of the Data Breach, at least one unidentified cybercriminal possesses the PII of Plaintiff and Class members. Now that the data is stolen, unidentified actors can exploit the PII for their own gain or sell the PII to others for a profit. With social security numbers and driver's license information, cybercriminals can open new bank accounts and take out loans. Actions like these can destroy the Plaintiff and Class members' credit scores, having damage on future attempts to borrow money, obtain credit, or open a bank account.

57. Cybercriminals can also use breached PII to obtain medical treatment using victim's health insurance, file false federal and state tax returns, and obtain government benefits. Victims of such identity theft are targeted by the IRS, added to credit fraud watch lists, and can be barred from making major purchases such as a new car or home.

58. The PII obtained during the Data Breach is highly valuable to cybercriminals for the aforementioned reasons.

59. In response to the Data Breach, T-Mobile offered affected customer offered two years of free identity protection services with McAfee's ID Theft Protection Services. However, two years is not enough time to effectively monitor one's credit after identity theft. Cybercriminals will often wait months or years after obtaining PII to use it. Plaintiff and Class members will have to diligently monitor their credit for years after the complimentary McAfee ID Theft Protection Services are up in order to ensure their PII obtained in the Data Breach is not used to harm them.

V. CLASS ACTION ALLEGATIONS

60. Plaintiff brings this nationwide class action pursuant to rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following class:

> All current, former, and prospective T-Mobile customers residing in the United States whose Private Information was compromised in the Data Breach announced by Defendant on or about August 16, 2021 (the "Nationwide Class").

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

61. Plaintiff also brings this class action individually and on behalf of all people in New York defined as follows:

> All current, former, and prospective T-Mobile customers residing in New York whose personal information was compromised as a result of the breach of T-Mobile US, Inc.'s information system(s) announced by Defendant on August 16, 2021. (the "New York Subclass")

62. The New York Subclass is referred to herein as the "New York Subclass" and together with the Nationwide Class, are collectively referred to herein as the "Classes."

63. Excluded from the Classes is Defendant, any entities in which Defendant has a controlling interest or that have a controlling interest in Defendant, and Defendant's legal representatives, assignees and successors. Also excluded are all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, and all judges assigned to this case and their immediate family members and staff.

64. **Numerosity.** The Classes are so numerous that joinder of all members is impracticable. Upon information and belief, the Nationwide Class consists of over 46 million customers whose data was compromised in the data breach. Membership in the classes is identifiable in Defendant's records

65. **Commonality and Predominance.** There are numerous questions of law and fact common to Plaintiff and Class members. These common questions predominate over any questions affecting only individual members of the Classes. The common questions of law and fact include, without limitation:

a. When Defendant actually learned of the Data Breach and whether its response was adequate;

b. Whether Defendant owed a duty to the Classes to exercise due care in collecting, storing, safeguarding and/or obtaining their Private Information;

c. Whether Defendant breached that duty;

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

d. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing the Private Information of Plaintiff and Members of the Classes;

e. Whether Defendant knew or should have known that it did not employ reasonable measures to keep the Private Information of Plaintiff and Members of the Classes secure and to prevent loss or misuse of that Private Information;

f. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

g. Whether Defendant caused Plaintiff's and Members of the Classes damage;

h. Whether Defendant violated the law by failing to promptly notify Plaintiff and Members of the Classes that their Private Information had been compromised;

i. Whether Defendant violated the consumer protection statutes invoked below; and

j. Whether Plaintiff and the other Members of the Classes are entitled to credit monitoring and other monetary relief.

66. **Typicality.** Plaintiff's claims are typical of the other Class Members because all members had Private Information compromised in the Data Breach and were harmed as a result.

67. **Adequacy.** Plaintiff will fairly and adequately represent and protect the interests of the Classes. Plaintiff has no interests that conflict with the interests of the Class she seeks to represent. Plaintiff's Counsel are competent and experienced in data breach class action litigation.

68. **Superiority.** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

individual prosecution of complex and expensive litigation. It would be very difficult, if not impossible, for members of the Class individually to effectively redress Defendant's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments.

69. Class certification is also appropriate under Rule 23(a) and (b)(2) because Defendant acted or refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Nationwide Class as a whole and/or as to the New York Subclass as a whole.

70. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Members of the Classes to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiff and the Members of the Classes to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

e. Whether members of the Classes are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

VI. FIRST CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiff, the Nationwide Class, and the New York Subclass)

71. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in the preceding paragraphs.

72. Defendant owed a common law duty to Plaintiff and Members of the Classes to exercise reasonable care in obtaining, using, and protecting their Private Information from unauthorized third parties.

73. The legal duties owed by Defendant to Plaintiff and Members of the Classes include, but are not limited to the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information of Plaintiff and Members of the Classes in its possession;

b. To protect Private Information of Plaintiff and Members of the Classes in its possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiff and Members of the Classes of the Data Breach.

74. Defendant's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a) (the "FTC Act"), which prohibits "unfair . . . practices in or affecting commerce," including, as interested and enforced by the Federal Trade Commission, the unfair practices by companies such as Defendant of failing to use reasonable measures to protect Private Information.

75. Various FTC publications and data security breach orders further form the basis of Defendant's duty. Plaintiff and Members of the Classes are consumers under the FTC Act. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

Private Information and by not complying with industry standards.

76. Defendant breached its duties to Plaintiff and Members of the Classes. Defendant knew or should have known the risks of collecting and storing Private Information and the importance of maintaining secure systems, especially in light of the fact that data breaches have been surging in the past 5 years.

77. Defendant knew or should have known that its security practices did not adequately safeguard the Private Information belonging to the Plaintiff and Members of the Classes.

78. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security and its failure to protect the Private Information of Plaintiff and Members of the Classes from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Private Information of Plaintiff and Members of the Classes during the period it was within Defendant's possession and control.

79. Defendant breached the duties it owed to Plaintiff and Members of the Classes in several ways, including:

a. Failing to implement adequate security systems, protocols, and practices sufficient to protect current, former, and prospective customers' Private Information, including Plaintiffs and Members of the Classes, and thereby creating a foreseeable risk of harm;

b. Failing to comply with the minimum industry data security standards prior to the Data Breach; and

c. Failing to act despite knowing or having reason to know that its systems were vulnerable to attack.

80. Due to Defendant's conduct, Plaintiff and Members of the Classes are entitled to credit monitoring. Credit monitoring is reasonable here. The Private Information taken can be used for identity theft and other types of financial fraud against Plaintiff and Members of the

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

Classes.

81. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach. Annual subscriptions for credit monitoring plans range from approximately $219 to $358 per year.[7]

82. As a result of Defendant's negligence, Plaintiff and Members of the Classes suffered injuries that may include: (i) the lost or diminished value of Private Information; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, time spent deleting phishing scams and reviewing and monitoring sensitive accounts; (iv) the present and continued risk to their Private Information, which may remain for sale on the dark web and is in Defendant's possession and subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession; (v) future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Members of the Classes, including ongoing credit monitoring.

83. These injuries were reasonably foreseeable given the history of security breaches of this nature. The injury and harm that Plaintiff and the members of the Classes suffered was the direct and proximate result of Defendant's negligent conduct.

VII. SECOND CLAIM FOR RELIEF
Negligence Per Se
(On Behalf of Plaintiff, the Nationwide Class, and the New York Subclass)

84. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in the preceding paragraphs.

[7] In the recent Equifax data breach, for example, Equifax agreed to free monitoring of victims' credit reports at all three major credit bureaus for four years, plus $1 million of identity theft insurance. For an additional six years, victims can opt for free monitoring by one credit bureau, Equifax. In addition, if a victim's child was a minor in May 2017, he or she is eligible for a total of 18 years of free credit monitoring under the same terms as for adults.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

85. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant's, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

86. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiff and Members of the Classes due to the valuable nature of the Private Information at issue in this case—including Social Security numbers.

87. Defendant's violations of Section 5 of the FTC Act constitute negligence per se.

88. Plaintiff and Members of the Classes are within the class of persons that the FTC Act was intended to protect.

89. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Members of the Classes.

90. As a direct and proximate result of Defendant's negligence per se, Plaintiff and Members Classes have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the present and continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of its current, former, and prospective customers in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Members of the Classes.

91. Additionally, as a direct and proximate result of Defendant's negligence per se, Plaintiff and Members of the Classes have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession.

VIII. THIRD CLAIM FOR RELIEF
Breach of Implied Contract
(On Behalf of Plaintiffs the Nationwide Class, and the New York Subclass)

92. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in the preceding paragraphs.

93. Defendant provided Plaintiff and Class Members with an implied contract to protect and keep confidential Defendant's current, former, and prospective customers' private, nonpublic personal and financial information when they gathered the information from each of their current, former, and prospective customers.

94. Plaintiff and Class Members would not have provided their personal and financial information to Defendant, but for Defendant's implied promises to safeguard and protect Defendant's current, former, and prospective customers private personal and financial information.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

95. Plaintiff and Class Members performed their obligations under the implied contract when they provided their private personal and financial information in exchange for telecommunication services provided by Defendant.

96. Defendant breached the implied contracts with Plaintiff and Class Members by failing to protect and keep private the nonpublic personal and financial information provided to them about Plaintiff and Class Members.

97. As a direct and proximate result of Defendant's breach of their implied contracts, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, damages and injuries.

IX. FOURTH CLAIM FOR RELIEF

Violation of the Washington State Consumer Protection Act (RCW 19.86.010 et seq.)
(On Behalf of Plaintiff and the Nationwide Class)

98. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in the preceding paragraphs.

99. The Washington State Consumer Protection Act, RCW 19.86.020 (the "CPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are described by the CPA and relevant case law.

100. Defendant is a "person" as described in RWC 19.86.010(1).

101. Defendant engages in "trade" and "commerce" as described in RWC 19.86.010(2) in that they engage in selling telecommunication products and services, that directly and indirectly affect the people of the State of Washington.

102. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the CPA, in that Defendant's practices were injurious to the public interest because they injured other persons, had the capacity to injure other persons, and have the capacity to injure other persons.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

103. In the course of conducting their business, Defendant committed "unfair or deceptive acts or practices" by, inter alia, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff and Class Members' Private Information, and violating the common law alleged herein in the process. Plaintiff and Class Members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

104. The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

105. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violations of the CPA, Plaintiff and Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*, (1) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (2) invasion of privacy; (3) breach of the confidentiality their Private Information; (5) deprivation of the value of their Private Information, for which there is a well-established national and international market; and/or (v) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages.

106. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of herself, Class Members, and the general public, also seeks restitution and an injunction prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to modify their corporate culture and design, adopt, implement, control, direct, oversee, manage,

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the Private Information entrusted to it.

107. Plaintiff, on behalf of herself and the Class Members also seek to recover actual damages sustained by each class member together with the costs of the suit, including reasonable attorney fees. In addition, the Plaintiff, on behalf of themselves and the Class Members request that this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each Class Member by three times the actual damages sustained not to exceed $25,000.00 per class member.

X. FIFTH CLAIM FOR RELIEF
Violation of the New York General Business Law §349
(On behalf of Plaintiff, the Nationwide Class and the New York Class)

108. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in the preceding paragraphs.

109. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a), including but not limited to the following:

a. Defendant misrepresented material facts to Plaintiff and Class members by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and Class members' PII from unauthorized disclosure, release, data breaches, and theft;

b. Defendant misrepresented material facts to Plaintiff and Class members by representing that it did and would comply with the requirements of federal and state laws pertaining to the privacy and security of Plaintiff's and Class members' PII;

c. Defendant omitted, suppressed, and concealed material facts of the inadequacy of its privacy and security protections for Plaintiff's and Class

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

members' PII; and

d. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Plaintiff's and Class members' PII, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45).

110. Defendant's failure constitutes false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiff and Class members) regarding the security of its network and aggregation of PII.

111. The misrepresentations upon which consumers (including Plaintiff and Class members) relied were material misrepresentations (e.g., as to Defendant's adequate protection of PII), and consumers (including Plaintiff and Class members) relied upon those representations to their detriment.

112. Defendant's conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead consumers acting reasonably under the circumstances. As a direct and proximate result of Defendant's conduct, Plaintiff and other Class members have been harmed, in that they were not timely notified of the data breach, which resulted in profound vulnerability to their personal information and other financial accounts.

113. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and omissions, Plaintiff's and Class members' PII was disclosed to third parties without authorization, causing and will continue to cause Plaintiff and Class members damages.

114. As a direct and proximate result of Defendant's violation of NY GBL §349, Plaintiff and Class members have suffered, and continue to suffer, injuries, damages arising from identity theft; from their needing to contact governmental agencies; potentially defending themselves from legal action base upon fraudulent use of their PII; contacting their financial institutions; loss of use of funds; closing or modifying financial accounts; damages from lost

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

time and effort to mitigate the actual and potential impact of the data breach on their lives; closely reviewing and monitoring their accounts for unauthorized activity which is certainly impending; placing credit freezes and credit alerts with credit reporting agencies; and damages from identity theft, which may take months or years to discover and detect.

XI. SIXTH CLAIM FOR RELIEF
Unjust Enrichment
(On Behalf of Plaintiff, the Nationwide Class, and the New York Subclass)

115. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in the preceding paragraphs.

116. Defendant benefited from receiving Plaintiff's and Members of the Classes' Private Information by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

117. Defendant also understood and appreciated that Plaintiff's and Members of the Classes' Private Information was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that Private Information.

118. Plaintiff's and Members of the Classes who were customers of Defendant's customer conferred a monetary benefit upon Defendant in the form of monies paid for services available from Defendant.

119. Defendant appreciated or had knowledge of the benefits conferred upon them by Plaintiff and members of the Classes. Defendant also benefited from the receipt of Plaintiff's and Members of the Classes' Private Information, as Defendant used it to facilitate the transfer of Private Information between parties.

120. The monies that Plaintiff's and Members of the Classes paid to Defendant for services were to be used by Defendant, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

121. Defendant also understood and appreciated that Plaintiff's and Members of the Classes' Private Information was private and confidential, and its value depended upon

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

Defendant maintaining the privacy and confidentiality of that Private Information.

122. But for Defendant's willingness and commitment to maintain privacy and confidentiality, that Private Information would not have been transferred to and entrusted with Defendant. Indeed, if Defendant had informed Plaintiff's and Members of the Classes that their data and cyber security measures were inadequate, Defendant would not have been permitted to continue to operate in that fashion by regulators, its shareholders, and its consumers.

123. As a result of Defendant's wrongful conduct, Defendant was unjustly enriched at the expense of, and to the detriment of, Plaintiff's and Members of the Classes. Defendant continues to benefit and profit from their retention and use of the Private Information while its value to Plaintiff's and Members of the Classes has been diminished.

124. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged in this Complaint, including compiling, using, and retaining Plaintiff's and Members of the Classes' Private Information, while at the same time failing to maintain that information secured from intrusion and theft by hackers and identity thieves.

125. As a result of Defendant's conduct, Plaintiff's and Members of the Classes suffered actual damages in an amount equal to the difference in value between the amount Plaintiff's and Members of the Classes paid for their purchases with reasonable data privacy and security practices and procedures and the purchases they actually received with unreasonable data privacy and security practices and procedures.

126. Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff's and Members of the Classes because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff's and Members of the Classes paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

127. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff's and Members of the Classes all unlawful or inequitable proceeds they received as a

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

result of the conduct alleged herein.

XII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment against Defendant as follows:

A. Certification of the Classes pursuant to Federal Rule of Civil Procedure 23;

B. Appoint Plaintiff Ania Villalon as representative of the Classes;

C. Appoint the undersigned counsel as counsel for the Classes;

D. That the Court award compensatory damages, punitive damages, statutory and civil penalties to Plaintiff and the Classes as warranted by all applicable laws alleged herein;

E. In the alternative, that the Court award nominal damages as permitted by law;

F. That the Court award injunctive or other equitable relief that directs Defendant to provide Plaintiff and the Classes with free credit monitoring and identity theft protection, and to implement reasonable security procedures and practices to protect customers' PII that conform to relevant federal and state guidelines and industry norms;

G. That the Court award declaratory judgment in favor of Plaintiff determining that Defendant's failure to implement reasonable security measures gives rise to a claim under the laws alleged herein;

H. Award Plaintiff and the Classes statutory, compensatory and exemplary damages as permitted by law;

I. Judgment against Defendant for attorney's fees and costs as permitted by law and/or equity;

J. Any other or further relief which the Court deems fair and equitable.

XIII. DEMAND FOR JURY TRIAL

Pursuant to Fed. R. Civ. P. 38(b), Plaintiff demands a trial by jury of all issues properly triable to a jury in this case.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

RESPECTFULLY SUBMITTED AND DATED this 24th day of August, 2021

TERRELL MARSHALL LAW GROUP PLLC

By: /s/ Beth E. Terrell, WSBA #26759
Beth E. Terrell, WSBA #26759
Email: bterrell@terrellmarshall.com
936 N. 34th Street, Suite 300
Seattle, Washington 98103
Telephone: (206) 206-816-6603
Facsimile: (206) 319-5450

Kevin Laukaitis*
Email: klaukaitis@shublawyers.com
Jonathan Shub*
Email: jshub@shublawyers.com
SHUB LAW FIRM LLC
134 Kings Highway East, 2nd Floor
Haddonfield, New Jersey 08033
Telephone: (856) 772-7200
Facsimile: (856) 210-9088

Attorneys for Plaintiff and the Classes

**Pro hac vice forthcoming*